

2:18-CR-00292-DWA

On October 28, 2018, the day after the date of the offense, the Government filed an Application for a search warrant pursuant to the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §§2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) pertaining to a certain Gab account with the user ID @onedingo (“Target Account”). (ECF No. 318-7, pp. 2-3). In support of the same, the Application detailed the offense at issue, including indications of planning and premeditation associated with the offense. *Id.* at pp. 1-18. In particular, the “FBI personnel searched a law enforcement database for BOWERS and learned that BOWERS is associated with the user name

'@onedingo.' An open source internet search revealed a screenshot of a post ...on a Gab account by an individual identified as ROBERT BOWERS with the username @onedingo." (ECF No. 318-7, p. 6).¹ The Application further provided as follows:

20. The Gab account contained an avatar comprised of a photo of BOWERS' face. The post contained an anti-Semitic comment and a reference to "going in" shortly before he entered the Synagogue and began shooting. Specifically, the post stated, "HIAS likes to bring invaders in that kill our people. I can't sit by and watch my people get slaughtered. Screw your optics. I'm going in."

Id.

As stated in the Application, the Government asked Gab to preserve Target Account information. *Id.* at pp. 6-7; *see also*, ECF No. 345-2/358-2. In the letter to Gab asking it to preserve the information, the Government advised Gab that it was "in the process of securing a court order, search warrant, and/or a subpoena for the production of records concerning the following username: onedingo....[W]e therefore wish that it be preserved until we have completed securing a court order and/or a subpoena for the production of records." (ECF No. 345-2/358-2, p. 1). Before the Government was able to secure the warrant, Gab responded by actually providing the information. *Id.* at pp. 6-7. Specifically, the Application provides:

21. On October 27, 2018, the FBI sent a preservation request to Gab asking that the @onedingo Gab Target Account be preserved. In response, and without being requested by the FBI, Gab provided the FBI with the contents of the Target Account. In a subsequent phone call with the founder of Gab, he confirmed that he voluntarily provided the contents of the Target Account to the FBI without being asked by the FBI to do so.

The Application further provides information on the Gab website regarding disclosure of information. *Id.* at p. 7.

22. Gab states on its website, as follows:

Information Disclosed for Our Protection and the Protection of Others.

¹Additionally, I note that the Government provided an FBI Import Form indicating that Andrew Torba, CEO of Gab.com, called the FBI Public Access Line at 11:30 a.m. on October 27, 2017, to advise the FBI that he thought the shooter in Pittsburgh was "an active user on gab.com." (ECF No. 345-1/358-1, p. 1). According to the Import Form, Torba learned of the Defendant's name by listening to a police scanner. *Id.* Torba stated that an hour before the shooting the Defendant made a post. *Id.* Torba also indicated that he suspended the account and archived the information. *Id.*

We cooperate with government and law enforcement officials or private parties to enforce and comply with the law. We may disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate: (i) to respond to claims, legal process (including subpoenas); (ii) to protect our property, rights and safety and the property, rights and safety of a third party or the public in general; and (iii) to stop any activity that we consider illegal or legally actionable activity.

Id.

The Government indicated that while Gab provided the contents of the Target Account voluntarily, “in an abundance of caution” it sought the warrant “to establish that the United States possessed probable cause to search the Target Account prior to receiving the contents from Gab.”

Id. The Government further provided that “[t]his material may have been viewed in the course of the investigation. However, material from Gab has been widely publicized by news media.” *Id.* The property to be searched and the particular items to be seized were detailed in Attachments A and B of the Application. *Id.* at pp. 12-15. On October 28, 2018, the Government obtained the warrant to search and seize “information associated with the Gab profile with username @onedingo at <http://Gab.com/onedingo> that is stored... by Gab....” (ECF No. 318-7, p. 1).

Analysis

The Defendant seeks to suppress evidence from Gab for the account with username @onedingo. *Id.* To that end, the Defendant raises two arguments: 1) there existed a reasonable expectation of privacy in the non-public information disclosed to the Government by Gab; and 2) the non-public information was seized and searched by the Government without first having obtained a warrant. (ECF No. 292/315). Specifically, the Defendant contends that the Government agents searched the non-public account information,² in which the Defendant had a reasonable expectation of privacy, without having first obtained a search warrant, in violation of

² The Defendant does not appear to challenge the public information provided by Gab as it specifically argues a reasonable expectation of privacy in the “non-public information disclosed to the government by Gab.com.” (ECF No. 292/315, p. 3-4). As a result, I find the Defendant’s Motion to Suppress No. 5 relates only to the non-public information disclosed by Gab to the Government and my discussion is limited accordingly.

the Fourth Amendment such that said information should be suppressed. *Id.* In opposition, the Government argues, *inter alia*, Gab provided the information voluntarily such that there was no governmental search and no Fourth Amendment violation and, therefore, no suppression is warranted. (ECF No. 345). Further, the Government argues that even if a warrant was necessary, it sought and obtained a valid search warrant to re-acquire the information based on probable cause “exclusive of the information voluntarily provided by Gab.com,” curing any issues. (ECF No. 345, p. 2).

To begin with, the Defendant maintains that he had a reasonable expectation of privacy in the non-public information disclosed by Gab and viewed by the Government without a warrant. (ECF No. 292/315, pp. 3-4). The Defendant argues that “[w]hile the Fourth Amendment may not bar the warrantless seizure of the public postings, it does bar the wholesale warrantless seizure of other information in which there existed a reasonable expectation of privacy.” (ECF No. 292/315, p. 3). In support of the same, the Defendant submits that he had a reasonable expectation of privacy in the non-public Gab information, suggesting, without more, that such information is “more akin to cell site location information,” which the Defendant argues requires a warrant, than to telephone call logs which the Defendant acknowledges does not require a warrant. (ECF No. 292/315, pp. 3-4). In so doing, the Defendant draws a “distinction between information that a person voluntarily discloses to a third party and information that the third party, without full notice, covertly collects for its own purposes and then later, as in this case, discloses to law enforcement.” *Id.* at 4.

Generally, the Fourth Amendment prohibits “unreasonable searches and seizures.” U.S. Const. Amend IV. The protection of the Fourth Amendment, however, pertains only to unreasonable searches and seizures conducted by government actors. *United States v. Jacobsen*, 466 U.S. 109, 113-114 (1984) (“This Court has also consistently construed this protection as proscribing only governmental action; it is wholly inapplicable ‘to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the

Government or with the participation or knowledge of any governmental official.” *Id.*, quoting *Walter v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)). Furthermore, as acknowledged by the Defendant, a person “has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). Along that same line, when a person is forewarned of the possible disclosure of information, courts have held privacy interests are not objectively reasonable. *United States v. Young*, 350 F.3d 1302, 1308 (11th Cir. 2003) (“No reasonable person would expect to retain his or her privacy interest in a packaged shipment after signing an airbill containing an explicit, written warning that the carrier is authorized to act in direct contravention that that interest.”); *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001); *United States v. Simon*, 206 F.3d 392, 398 (4th Cir. 2000) (Defendant “did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy....This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private.” Thus, defendant did not have an objectively reasonable expectation of privacy after being advised of the internet policy.). Thus, courts have held that a governmental “viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment...It infringed no legitimate expectation of privacy and hence was not a ‘search’ within the meaning of the Fourth Amendment.” *Jacobsen*, 466 U.S. at 119-120, citing *Coolidge v. New Hampshire*, 403 U.S. 443, 487-490 (1971).

Despite the Defendant’s contentions, I need not discuss in great detail (or conduct a hearing on) whether the Defendant had a reasonable expectation of privacy in the non-public information held by Gab,³ whether the Defendant was adequately forewarned of the possible

³The Defendant argues that he has a privacy expectation in the non-public information maintained by Gab, which is administrative in nature (e.g. the timing of the post or that fact that it was made from an Android phone). In reviewing such information, however, I note that courts have held that routine subscriber records and account information provided to an internet provider is not protected by the Fourth Amendment. See, *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (complying cases). “Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.” *Id.* at 1204 (complying cases). In *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010), the Third Circuit, citing *Perrine*, held that a defendant “had no reasonable expectation of privacy in his IP address and so cannot establish a Fourth

disclosure of the information by Gab,⁴ or if Gab's disclosure was protected by the ECPA⁵ because suppression is not warranted regardless of these issues pursuant to the good faith exception to exclusionary rule.⁶ In other words, even if the subject evidence was improperly produced by Gab and/or was improperly seized by the Government prior to the issuance of a warrant, suppression or exclusion of the subject evidence not is automatic. *Herring v. United States*, 555 U.S. 135, 137 (2009) ("[S]uppression is not an automatic consequence of a Fourth Amendment violation."). The

Amendment violation." See also, *United States v. Stanley*, Cr. No. 11-272, 2010 WL 5512987, at *12-17 (W.D. Pa. Nov. 14, 2012), *aff'd* 753 F.3d 114 (3d Cir. 2014), *cert. denied*, 574 U.S. 1003 (2014) ("An internet subscriber does not have a reasonable expectation of privacy in his IP address or the information he provides to his Internet Service Provider....").

⁴ Again, according to the Application for the warrant, Gab provides the following disclosure:

22. Gab states on its website, as follows:

Information Disclosed for Our Protection and the Protection of Others.

We cooperate with government and law enforcement officials or private parties to enforce and comply with the law. We may disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate: (i) to respond to claims, legal process (including subpoenas); (ii) to protect our property, rights and safety and the property, rights and safety of a third party or the public in general; and (iii) to stop any activity that we consider illegal or legally actionable activity.

(ECF No. 318-7 at p. 7).

⁵ Pursuant to the ECPA, a person or entity providing an electronic communication service to the public may divulge the contents of a communication or a record or other information pertaining to the subscriber or customer to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure." 18 U.S.C. §2702(b)(8) and (c)(4).

⁶ The Defendant argues that the information obtained from Gab's disclosure was used in obtaining another warrant (for the Target cell phone) prior to obtaining the warrant at issue here. To that end, the Defendant specifically points to paragraph 20 of the application for the Target cell phone. Reviewing the application for the Target cell phone, however, I note that application merely cites that "[r]ecords were obtained by the FBI from a social media site that included an anti-Semitic post on Bowers' account" and that the "post was made from an Android phone at 13:49 UTC on October 27, 2018." (ECF No. 318-7, p. 26, ¶20). As to the type of phone, the Application explicitly states that "[o]pen source information confirms that LG model G6 Cell phones are Android phones." (ECF No. 318-7, p. 26, ¶19). With regard to the time of the post, such information is non-content information. As discussed in a prior footnote, information that is non-content and administrative in nature, like subscriber and IP information, do not implicate privacy interests as they are maintained by third parties. See, *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (complying cases); *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010); *United States v. Stanley*, Cr. No. 11-272, 2010 WL 5512987, at *12-17 (W.D. Pa. Nov. 14, 2012), *aff'd* 753 F.3d 114 (3d Cir. 2014), *cert. denied*, 574 U.S. 1003 (2014).

goal of the exclusionary rule is to deter Fourth Amendment violations. *Id.* at 139-140; *see also*, *United States v. Werdene*, 883 F.3d 204, 215 (3d Cir. 2018). Exclusion is a “last resort, not our first impulse.” *Id.* at 140; *U.S. v. Caesar*, No. 19-3961, 2021 WL 2559471, at *6 (3d Cir. June 23, 2021)(“Exclusion is a ‘bitter pill’ swallowed only where it would result in a ‘substantial deterrent effect’ that outweighs its resulting costs, [*U.S. v.*] *Leon*, 486 U.S. [897] at 907 [1984].”). Accordingly, if officers acted with an “objectively reasonable good-faith belief that their conduct [was] lawful or when their conduct involve[d] only simple, isolated negligence,” there is no deterrent effect justifying exclusion of evidence. *United States v. Katzin*, 769 F.3d 163, 171 (3d Cir. 2013); *Caesar*, 2021 WL 2559471 at *6. Thus, “to trigger the exclusionary rule, law enforcement conduct must be ‘deliberate, reckless, or grossly negligent,’ or involve ‘recurring or systemic negligence.’” *Caesar*, 2021 WL 2559471 at *6, *quoting*, *Herring*, 555 US at 143-44. Therefore, the good faith inquiry rests on “‘the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal’ in light of ‘all of the circumstances.’” *United States v. Horton*, 863 F.3d 1041, 1051 (8th Cir. 2017), *quoting*, *Herring*, 555 U.S. at 145.

In this case, there is no evidence that the Government acted to have Gab reveal or in any way provide the information. To be clear, the letter from the Government to Gab cites to the ECPA and asks Gab to “preserve” the information “until we have completed securing a court order.” (ECF No. 345-2/358-2). Thus, the sentence in the letter stating that “[w]illful failure to comply with this request may subject you to prosecution for obstruction of justice,” cannot be reasonably read as a demand to turn over the information to the Government as the Defendant seems to suggest. Rather, the Government sought to have the information preserved while it was seeking a warrant. Nonetheless, assuming for the sake of argument that there was a Fourth Amendment violation, the fact remains that the warrant was issued after a review by a magistrate judge. (ECF No. 318-7, p.. 1-18). It is important to note, Defendant is not challenging the sufficiency or validity of the warrant that incorporates the offenses under investigation and outlines

the property to be searched and the particular things to be seized. Therefore, I find suppression would have no appreciable deterrent effect. Consequently, even if there was a Fourth Amendment violation, I find the good faith exception to the exclusionary rule applies and suppression is not warranted.

Furthermore, even if the good faith exception to the exclusionary rule did not apply, suppression still is not justified here. While the warrant came after the disclosure by Gab,⁷ that does not negate the fact that a valid warrant for the information was obtained such that the information would have been inevitably discovered by lawful means⁸ and/or through an independent source.⁹ Therefore, I find suppression of the information obtained from Gab is not warranted pursuant to the Fourth Amendment as requested by the Defendant.¹⁰

An appropriate order shall follow.

⁷ There is no question that Gab's CEO contacted the FBI and provided the information to the FBI before the Government obtained the warrant. Further, there is no evidence that the Government looked beyond the scope of the information provided by Gab before obtaining the warrant. *See, Jacobsen*, 466 U.S. at 119-120 (An "agent's viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment."), *citing, Coolidge v. New Hampshire*, 403 U.S. 443, 487-490 (1971).

⁸ Pursuant to the inevitable discovery rule, "if the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means...then the deterrence rationale has so little basis that the evidence should be received." *United States v. Vasquez De Reyes*, 149 F.3d 192, 195 (3d Cir. 1998) *citing Nix v. Williams*, 467 U.S. 431, 444 (1984). In this case, the information displayed on the Defendant's Gab account would have been inevitably discovered as it was widely captured and disseminated by the media on October 27, 2018. Additionally, the Government sought and subsequently obtained a warrant from a magistrate judge for the information the Defendant is seeking to suppress. (ECF No. 318-7, pp. 1-18). Again, the Defendant does not contest the validity of said warrant.

⁹ Exclusion of evidence is not warranted if the Government has an independent source of the evidence sought to be suppressed. *Murray v. United States*, 487 U.S. 533, 537 (1988); *see also United States v. Herrold*, 962 F.2d 1131, 1144 (3d Cir. 1992). "The underlying rationale for the independent source rule is that the exclusionary rule ensures that the police should not be in a better position as a result of their illegal action, but neither should they lie in a worse position." *United States v. Vasquez De Reyes*, 149 F.3d 192, 194 (3d Cir. 1998). In this case, the Government sought and subsequently obtained a warrant from a magistrate judge for the information the Defendant is seeking to suppress. (ECF No. 318-7, pp. 1-18). Again, the Defendant does not contest the validity of said warrant. Consequently, I find the information was validly obtained by an independent source and should not be excluded.

¹⁰ In his Reply to the Government's Opposition, the Defendant seeks an evidentiary hearing. (ECF No. 379/389). Based on the discussion above, I find a hearing is not necessary.

